UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

VIRTRU CORPORATION,

Plaintiff,

v.

MICROSOFT CORPORATION,

Defendant.

Case No. 6:22-cv-00242

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Virtru Corporation ("Virtru"), by and through its undersigned counsel, files this Complaint against Defendant Microsoft Corporation ("Microsoft") and alleges as follows:

1. Virtru brings this action for patent infringement under the patent laws of the United States, Title 35 of the United States Code, against Microsoft for its infringement of Virtru's United States Patent No. 8,589,673 (the "'673 Patent"), United States Patent No. 8,874,902 (the "'902 Patent"), and United States Patent No. 9,578,021 (the "'021 Patent") (collectively, the "Patents-in-Suit").

2. Virtru is a leading data protection and privacy company founded by brothers John Ackerly and Will Ackerly in 2012. Today, Virtru serves more than 7,300 customers, including Fortune 50 companies, government agencies, financial institutions, hospitals, and leading universities. Virtru's products help these customers protect data as it is moved or shared using email applications, file-sharing platforms, software-as-a-service apps, and cloud environments. Since its founding, Virtru's products have protected more than one billion data assets and they

currently secure nearly two million emails and files every day.

3. The Ackerly brothers founded Virtru based on their vision and belief that easy, secure data-sharing would be essential to the digital economy. Both brothers experienced this unmet need firsthand while working in national security.

4. Before founding Virtru, John worked as a White House policy director during the terrorist attacks on September 11, 2001, and saw how secure data sharing could have helped connect the dots between the intelligence data stored in disparate locations and stop the attacks before they happened.

5. Will worked as a Cloud Security Architect at the National Security Agency for over eight years, where he was in charge of protecting the NSA's in-house data transfers. While at the NSA, Will saw how difficult it was to share sensitive data securely. For example, when he was deployed in Iraq, Will often had to run hundreds of yards to physically deliver USB sticks carrying sensitive information to special ops teams, as that was the only way to securely transfer data.

6. Determined to help the intelligence community share sensitive data securely, Will invented the Trusted Data Format ("TDF"). Unlike the traditional network-based approach to data security, TDF brought control back to the data itself and protects the data throughout its lifespan and wherever it travels. And in contrast to most encryption methods, TDF is universal: it works for any type of data and across any cloud environment or device. Realizing that this innovative approach to encryption could make a much larger impact beyond the intelligence community, Will and John founded Virtru to empower people and organizations of all sizes to easily and securely share sensitive data.

7. Since Virtru's founding, Will has invented proprietary technologies that simplify

the experience of creating, sharing, and accessing protected data that ensure a seamless user experience for Virtru's customers. Will invented the technologies embodied in the Patents-in-Suit, which claim methods and systems for distributing cryptographic data to authenticated recipients via secured or unsecured channels. This patented technology allows users to share encrypted information securely (e.g., via email or file-sharing platforms) without requiring a new username or password to access it. Virtru's technology "recognizes" the recipient and allows them to decrypt the information using existing credentials from another service—Google, for example—seamlessly and without creating a new account.

8. Without a license or authorization, Microsoft is employing these patented Virtru technologies in an ever-growing number of products and services, including its flagship Microsoft Office365 and Microsoft Azure products, causing irreparable harm to Virtru's business. On information and belief, Microsoft is using its substantial footprint in this district—which includes multiple data centers and corporate sales offices—in furtherance of this infringement.

9. Virtru brings this lawsuit to enforce its patent rights and prevent Microsoft from unfairly profiting from Virtru's inventions.

PARTIES

10. Virtru is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business at 1130 Connecticut Avenue, N.W. #210, Washington, D.C. 20036.

11. Virtru offers a range of innovative data protection products, including Gmail Encryption, Google Drive Encryption, Outlook Encryption, Enterprise Applications, and Trusted Data Platform, which provide encryption, access controls, key management, and persistent audit solutions. Virtru's intellectual property portfolio covers its novel innovations in data protection

and encryption key management technologies, which enable customers to share sensitive information securely.

12. On information and belief, Microsoft is a corporation organized and existing under the laws of the State of Washington, with a principal place of business in this district located at 10900 Stonelake Boulevard, Suite 225, Austin, Texas 78759.[1]

JURISDICTION AND VENUE

13. This action arises under the patent laws of the United States, 35 U.S.C. § 1 *et seq.*, including 35 U.S.C. §§ 271, 281, 283, 284, and 285. This Court has subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

14. Microsoft is subject to this Court's personal jurisdiction under the Texas Long Arm Statute and federal due process requirements because it has committed acts within Texas and within this district giving rise to this action, is registered to do business within the district, and has maintained established places of business having contacts within the state of Texas and within this district. Through its physical, regular, established places of business, on information and belief, Microsoft regularly conducts business in this district, including (i) purposefully and voluntarily placing one or more infringing products into the stream of commerce with the expectation that they will be purchased by consumers in this district; (ii) regularly conducting or soliciting business, engaging in a persistent course of business, employing people, or deriving substantial revenue through the sale and licensing of goods and services including the sale and use of the Accused Products in this district; and (iii) otherwise availing itself of the privileges and benefits of doing business in the state of Texas and within this district.

15. On information and belief, Microsoft conducts business within the State of Texas

[1] *Microsoft U.S. office locations*, Microsoft, https://www.microsoft.com/en-us/about/officelocator?Location=76501.

and in this district, and has designated Corporation Service Company d/b/a CSC − Lawyers Incorporating Service Company, 211 E. 7th Street, STE 620, Austin, Texas 78701-3218, as its agent for service of process in this district.

16. On information and belief, Microsoft has been registered to do business within the State of Texas under Texas Secretary of State File Number 0010404606 since about March 1987.

17. On information and belief, Microsoft derives substantial revenue through the sale and licensing of goods and services in this district, including the Accused Products, through its corporate sales offices in this district, including its corporate sales offices located at: 10900 Stonelake Boulevard, Suite 225, Austin, Texas 78759, and Concord Park II, 401 East Sonterra Boulevard, Suite 300, San Antonio, Texas 78258.[2]

18. On information and belief, Microsoft employs one or more of its data centers in this district in furtherance of infringing acts in this district. For example, Microsoft maintains data centers in this district, located at: 5150 Rogers Road, San Antonio, Texas 78251; 3823 Wiseman Boulevard, San Antonio, Texas 78251; and 5200 Rogers Road, San Antonio, Texas 78251.[3]

19. On information and belief, Microsoft has operated data centers supporting Microsoft products and services within the State of Texas, and within this district, since at least 2008.[4] Microsoft is building at least three additional data centers in this district, including two data centers located at: 3545 Wiseman Boulevard, San Antonio, Texas 78251, and another data center located at 15000 Block Lambda Drive, San Antonio, Texas 78245.[5] Upon information and

---

[2] *Id.*
[3] *San Antonio – Microsoft Reaches Mid-Point on $86M Expansion in Westover Hills*, Microsoft (Jan. 31, 2020), https://www.virtualbx.com/industry-news/san-antonio-microsoft-reaches-mid-point-on-86m-expansion-in-westover-hills/.
[4] *See* https://azure.microsoft.com/en-us/global-infrastructure/geographies/#geographies; https://www.datacenterknowledge.com/archives/2008/09/22/microsoft-makes-san-antonio-a-force.
[5] SBG San Antonio Staff Reports, *Microsoft to spend more than $200 million on data centers in San Antonio* NEWS4SA (Jul. 13, 2021), https://news4sanantonio.com/news/local/reports-microsoft-to-spend-more-than-200-million-on-data-centers-in-san-antonio; Data Center Dynamics, *Microsoft to build another data center in San*

belief, Microsoft's data centers, including those in this district, include computer hardware (*e.g.*, memory and processors) that store and execute at least portions of Microsoft's infringing software.

20. On information and belief, Microsoft has employed, is employing, and is offering to employ individuals in this district in furtherance of infringing acts in this district. On information and belief, these employees have direct personal knowledge about the Accused Products and Microsoft's infringing activities.

21. On information and belief, one or more of the Accused Products are used, offered for sale, and sold in this district, including by Microsoft and by "Microsoft-certified resellers" (e.g., Heart of Texas Network Consultants, located at 703 Willow Grove Rd., Waco, Texas 76712).[6]

22. Venue is proper in the Western District of Texas pursuant to 28 U.S.C. §§ 1391 and 1400(b) because Microsoft maintains regular and established places of business in this district and has committed acts of infringement within this district giving rise to this action.

THE PATENTS-IN-SUIT

23. The Patents-in-Suit claim methods and systems for distributing cryptographic data to authenticated recipients via secured or unsecured channels.

24. The '673 Patent, entitled "Methods and Systems for Distributing Cryptographic Data to Authenticated Recipients," duly and legally issued on November 19, 2013, from U.S. Patent Application No. 13/340,732, filed on December 30, 2011, naming William Rodgers Ackerly as the inventor. This application claims priority to U.S. Provisional Patent Application No. 61/432,181, filed on January 12, 2011. A true and correct copy of the '673 Patent is attached

Antonio, Texas (Apr. 6, 2021), https://www.datacenterdynamics.com/en/news/microsoft-to-build-another-data-center-in-san-antonio-texas/.

[6] *See* https://hotnc.com/it-services/software-services/microsoft-partner-network.html.

hereto as Exhibit A and is incorporated by reference.

25. The '902 Patent, entitled "Methods and Systems for Distributing Cryptographic Data to Authenticated Recipients," duly and legally issued on October 28, 2014 from U.S. Patent Application No. 14/064,274, filed on October 28, 2013, naming William Rodgers Ackerly as the inventor. This application is a continuation of and claims priority to U.S. Patent Application No. 13/340,732, filed on December 30, 2011; which claims priority to U.S. Provisional Patent Application No. 61/432,181, filed on January 12, 2011. A true and correct copy of the '902 Patent is attached hereto as Exhibit B and is incorporated by reference.

26. The '021 Patent, entitled "Methods and Systems for Distributing Cryptographic Data to Authenticated Recipients," duly and legally issued on February 21, 2017 from U.S. Patent Application No. 14/949,087, filed on November 23, 2015, naming William Rodgers Ackerly as the inventor. This application is a continuation of and claims priority to U.S. Patent Application No. 14/489,604, filed on September 18, 2014; which is a continuation of and claims priority to U.S. Patent Application No. 14/064,274, filed on October 28, 2013; which is a continuation of and claims priority to U.S. Patent Application No. 13/340,732, filed on December 30, 2011; which claims priority to U.S. Provisional Patent Application No. 61/432,181, filed on January 12, 2011. A true and correct copy of the '021 Patent is attached hereto as Exhibit C and is incorporated by reference.

27. Virtru is the owner and assignee of all right, title, and interest in and to the Patents-in-Suit, including the right to assert all causes of action arising under said patents and to seek damages and any other remedies for infringement of them.

THE ACCUSED PRODUCTS

28. The "Accused Products" are Microsoft products, systems, and/or services that

include infringing encryption and rights management technology.

29. Microsoft's infringing message encryption and rights management technology includes at least three technologies available in many Microsoft products, systems, and services: the Office 365 Message Encryption feature ("OME"); the Azure Portal feature used in combination with the Azure Active Directory B2B feature ("AP"); and the Azure Key Vault feature used in combination with the Azure Active Directory B2B feature ("AKV").[7]

30. On information and belief, the OME feature is included in at least the following Microsoft products, systems, or services: Office 365 Enterprise E3, Office 365 Enterprise E5, Microsoft 365 Enterprise E3, Microsoft 365 Enterprise E5, Microsoft 365 Business Premium, Office 365 A1, Office 365 A3, Office 365 A5, Microsoft 365 A1 (legacy), Microsoft 365 A1 for devices, Microsoft 365 A3, Microsoft 365 A5, Office 365 Government G3, Office 365 Government G5, Exchange Server 2013, Exchange Server 2016, Azure Information Protection Premium P1, Azure Information Protection Premium P2, Azure Information Protection for Office 365, Microsoft 365 Family, Microsoft 365 Personal, Outlook.com, Outlook for Microsoft 365, Outlook 2019, Outlook 2016, Outlook 2013, Outlook 2010, and Outlook 2007.[8] On information and belief, Microsoft also makes OME available as an add-on to additional Microsoft products and services, including: Exchange Online Plan 1, Exchange Online Plan 2, Exchange Online

[7] *Introducing Office 365 Message Encryption: Send encrypted emails to anyone!*, Microsoft (Nov. 21, 2013), https://www.microsoft.com/en-us/microsoft-365/blog/2013/11/21/introducing-office-365-message-encryption-send-encrypted-emails-to-anyone/; *Encrypt email messages*, Microsoft, https://support.microsoft.com/en-us/office/encrypt-email-messages-373339cb-bf1a-4509-b296-802a39d801dc; *Office 365 Message Encryption*, Microsoft, https://www.microsoft.com/en-us/microsoft-365/exchange/office-365-message-encryption; *B2B collaboration overview*, Microsoft (Feb. 20, 2022), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b; *Azure portal overview*, Microsoft (Aug. 30, 2021), https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-overview; *About Azure Key Vault*, Microsoft (Oct. 18, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/overview.

[8] *Message Encryption FAQ*, Microsoft (May 22, 2020), https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide#who-can-use-ome-; *Exchange Online service description*, Microsoft (Feb. 10, 2022), https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-service-description.

Kiosk, Microsoft 365 F1, Microsoft 365 Business Basic, Microsoft 365 Business Standard, and Office 365 Enterprise E1.[9] This list is based on publicly available information, and is preliminary and non-limiting. On information and belief, other Microsoft products, systems, and services related to Office 365 may also include OME or other infringing message encryption and rights management technology, including: Microsoft 365 Apps for business, Microsoft 365 Apps for enterprise (formerly Office 365 ProPlus), Office 365 Government G1, SharePoint Online Plan 1, Office 365 F3, and Microsoft 365 F3.

31. Upon information and belief, Microsoft's data centers, including those in this district, include computer hardware (*e.g.*, memory and processors) that store and execute at least portions of Microsoft's infringing OME software.[10] On information and belief, at least a portion of OME functions are performed in data centers located within this district.

32. On information and belief, the AP feature is included in at least the following Microsoft products, systems, or services: Azure Active Directory Premium Plan 1, Azure Active Directory Premium Plan 2, Microsoft 365 Enterprise E3, Microsoft 365 Enterprise E5, Microsoft 365 A3, Microsoft 365 A5, Microsoft 365 Government G3, Microsoft 365 Government G5, Microsoft 365 F1, Microsoft 365 F3, Enterprise Mobility & Security E3, Enterprise Mobility & Security E5, Microsoft 365 E5 Security, Microsoft 365 F5 Security, Microsoft 365 F5 Security & Compliance, and Microsoft 365 Business Premium.[11] On information and belief, Microsoft also makes AP available as an add-on to additional Microsoft products and services, including: Azure

[9] *Id.*
[10] *Microsoft Azure's southern U.S. data center goes down for hours, impacting Office365 and Active Directory customers*, https://www.geekwire.com/2018/microsoft-azures-southern-u-s-data-center-goes-hours-impacting-office365-active-directory-customers/
[11] *Azure Active Directory External Identities pricing*, Microsoft, https://azure.microsoft.com/en-us/pricing/details/active-directory/external-identities/; *Microsoft 365 guidance for security & compliance*, Microsoft (Dec.28, 2021), https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance#azure-active-directory-identity-protection.

Active Directory Free, Azure, Dynamics 365, Intune, Power Platform, Office 365 E1, Office 365 E3, Office 365 E5, and Office 365 F3.[12] This list is based on publicly available information, and is preliminary and non-limiting. On information and belief, other Microsoft products, systems, and services related to Azure may also include AP or other infringing message encryption and rights management technology, including: Office 365 A1, Office 365 A3, Office 365 A5, Microsoft 365 A1 (legacy), and Microsoft 365 A1 for devices.

33. Upon information and belief, Microsoft's data centers, including those in this district, include computer hardware (*e.g.*, memory and processors) that store and execute at least portions of Microsoft's infringing AP software.[13] On information and belief, at least a portion of AP functions are performed in data centers located within this district.

34. On information and belief, the AKV feature is included in at least the following Microsoft products, systems, or services: Azure Key Vault Standard, Azure Key Vault Premium, Azure Active Directory Premium Plan 1, Azure Active Directory Premium Plan 2, Microsoft 365 Enterprise E3, Microsoft 365 Enterprise E5, Microsoft 365 A3, Microsoft 365 A5, Microsoft 365 Government G3, Microsoft 365 Government G5, Microsoft 365 F1, Microsoft 365 F3, Enterprise Mobility & Security E3, Enterprise Mobility & Security E5, Microsoft 365 E5 Security, Microsoft 365 F5 Security, Microsoft 365 F5 Security & Compliance, and Microsoft 365 Business Premium.[14] On information and belief, Microsoft also makes AKV available as an add-on to

[12] *Azure Active Directory Pricing*, Microsoft, https://www.microsoft.com/en-us/security/business/identity-access-management/azure-ad-pricing?rtc=1#coreui-contentrichblock-gtwdiwu.

[13] *Microsoft Azure's southern U.S. data center goes down for hours, impacting Office365 and Active Directory customers*, https://www.geekwire.com/2018/microsoft-azures-southern-u-s-data-center-goes-hours-impacting-office365-active-directory-customers/

[14] *Azure Active Directory External Identities pricing*, Microsoft, https://azure.microsoft.com/en-us/pricing/details/active-directory/external-identities/; Microsoft 365 guidance for security & compliance, Microsoft (Dec.28, 2021), https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance#azure-active-directory-identity-protection; *Key Vault pricing*, Microsoft, https://azure.microsoft.com/en-us/pricing/details/key-vault/.

additional Microsoft products and services, including: Azure Active Directory Free, Azure, Dynamics 365, Intune, Power Platform, Office 365 E1, Office 365 E3, Office 365 E5, and Office 365 F3.[15] This list is based on publicly available information, and is preliminary and non-limiting. On information and belief, other Microsoft products, systems, and services related to Azure may also include AKV or other infringing encryption and rights management technology, including: Office 365 A1, Office 365 A3, Office 365 A5, Microsoft 365 A1 (legacy), and Microsoft 365 A1 for devices.[16]

35. Upon information and belief, Microsoft's data centers, including those in this district, include computer hardware (*e.g.*, memory and processors) that store and execute at least portions of Microsoft's infringing AKV software.[17] On information and belief, at least a portion of AKV functions are performed in data centers located within this district.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 8,589,673

36. Virtru incorporates herein by reference the allegations stated above in paragraphs 1–35 of this Complaint.

37. On information and belief, Microsoft has been and is now directly infringing the '673 Patent in this district and elsewhere, in violation of 35 U.S.C. § 271(a) at least by making, using, selling, offering for sale, and/or importing into the United States, Accused Products that practice one or more claims of the '673 Patent, including at least claim 1.

38. Microsoft has committed infringing acts without the permission, consent,

[15] *Azure Active Directory Pricing*, Microsoft, https://www.microsoft.com/en-us/security/business/identity-access-management/azure-ad-pricing?rtc=1#coreui-contentrichblock-gtwdiwu.
[16] https://azure.microsoft.com/en-us/global-infrastructure/services/?products=key-vault
[17] *Microsoft Azure's southern U.S. data center goes down for hours, impacting Office365 and Active Directory customers*, https://www.geekwire.com/2018/microsoft-azures-southern-u-s-data-center-goes-hours-impacting-office365-active-directory-customers/

authorization, or license of Virtru.

39. Microsoft's infringement is literal, under the doctrine of equivalents, or both.

40. On information and belief, Microsoft has been and is now indirectly infringing the '673 Patent in violation of 35 U.S.C. § 271(b) at least by inducing its customers to purchase the Accused Products and/or by instructing, encouraging, and/or directing others how to use the Accused Products in ways that directly infringe at least claim 1 of the '673 Patent.

41. On information and belief, by using the Accused Products as encouraged and directed by Microsoft, Microsoft's customers directly infringe one or more claims of the '673 Patent, including at least claim 1. For example, through its product manuals, sales and marketing activities, support activities, and other materials and activities, Microsoft solicits, instructs, encourages, and aids and abets its customers to purchase and use the Accused Products in infringing ways.[18]

42. Microsoft has had knowledge of the '673 Patent and its infringement of the '673 Patent since at least service of this Complaint.

43. Furthermore, on information and belief, Microsoft knew or was at least willfully blind to the existence of the '673 Patent and its infringement of the '673 Patent.

44. These facts give rise to a reasonable inference that Microsoft has knowingly induced its customers to infringe at least claim 1 of the '673 Patent directly, and that Microsoft has possessed a specific intent to cause such direct infringement. Further discovery may reveal earlier or additional knowledge of the '673 Patent, which would provide additional evidence of

[18] *See, e.g.*, *Message Policy and Compliance: Office 365 Message Encryption*, Microsoft (Apr. 8, 2021), https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/message-policy-and-compliance?redirectedfrom=MSDN#bkmk_O365_MessageEncryption; Microsoft Ignite, *Protect and control your sensitive emails with new Office 365 Message Encryption capabilities*, YouTube (Sept. 28, 2017), https://www.youtube.com/watch?v=R3cDOFXToNQ&t=1087s.

Microsoft's intent to induce infringement.

45. Microsoft's infringement of the '673 Patent has been and continues to be deliberate and willful, and this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees and costs pursuant to 35 U.S.C. §§ 284 and 285.

46. On information and belief, Microsoft lacks a good faith belief that the claims of the '673 Patent are not infringed, invalid, or unenforceable.

47. On information and belief, Microsoft will continue to infringe the '673 Patent, causing irreparable harm for which there is no adequate remedy at law, unless enjoined by this Court. On information and belief, Microsoft's infringement of the '673 Patent has caused and continues to cause irreparable harm to Virtru, including in this district, in the form of, among other things, loss of market share; price erosion; lost business opportunities and sales; loss of goodwill associated with Virtru's innovative technologies; entry into the market of additional infringers; and loss of its exclusive right to license its invention.

48. As a result of Microsoft's infringement of the '673 Patent, Virtru has suffered and is owed monetary damages adequate to compensate it for the infringement under 35 U.S.C. § 284, but in no event less than a reasonable royalty.

49. Microsoft and its customers infringe at least claim 1 of the '673 Patent as set forth below.[19]

Infringement of Claim 1 of the '673 Patent by Accused Products with OME

50. Claim 1 of the '673 Patent discloses a method for sharing secure information with authenticated recipients, in which the authentication is performed by an identity provider that is automatically selected based on information about the authorized recipients.

[19] Certain claim language in the '673 patent was corrected through certificates of correction issued by the USPTO on February 18, 2014, November 17, 2020, May 11, 2021, and February 22, 2022.

51. Microsoft's OME feature is a service that allows users to share encrypted email messages with authenticated recipients, where authentication is performed by an identity provider (e.g., a third-party service such as Google or Yahoo) that is automatically selected based on information about the authorized recipients (e.g., the recipient's email address). The Accused Products with the OME feature employ the method of at least claim 1 of the '673 Patent for sharing secure information with authenticated recipients.

52. On information and belief, the Accused Products with OME practice a method for distributing cryptographic data to authenticated recipients via secured or unsecured channels. For example, on information and belief, the Accused Products with OME "allow[] email users to send encrypted email messages to anyone," which "provide enhanced end user experiences that make it easier to share and collaborate on protected messages with anyone inside or outside the organization."[20]

53. On information and belief, the Accused Products with OME receive, by an access control management system (*e.g.*, Microsoft server), from a first client device (*e.g.*, an email creator's device using Microsoft Office 365), information associated with an encrypted data object (*e.g.*, the metadata associated with the encrypted email).[21]

54. On information and belief, the Accused Products with OME receive, by the access control management system (*e.g.*, Microsoft server), from a second client device (*e.g.*, an email recipient's device), a request for the information associated with the encrypted data object (*e.g.*, a recipient clicks "Read the message" button, thereby sending a request to the Microsoft server to

[20] *Message Policy and Compliance: Office 365 Message Encryption*, Microsoft (Apr. 8, 2021), https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/message-policy-and-compliance?redirectedfrom=MSDN#bkmk_O365_MessageEncryption.

[21] Microsoft Ignite, *Protect and control your sensitive emails with new Office 365 Message Encryption capabilities*, YouTube (Sept. 28, 2017), https://www.youtube.com/watch?v=R3cDOFXToNQ&t=1087s.

access the metadata associated with the encrypted email).[22]

55. On information and belief, the Accused Products with OME verify, by the access control management system (*e.g.*, Microsoft server), that a user of the second client device (*e.g.*, an email recipient) is identified in the received information associated with the encrypted data object (*e.g.*, Microsoft server verifies that the email recipient's email is included in the metadata associated with the encrypted email).[23]

56. On information and belief, the Accused Products with OME automatically select, by the access control management system (*e.g.*, Microsoft server), an identity provider from a plurality of identity providers (*e.g.*, third-party service such as Google or Yahoo), based on a user identifier included in the received information associated with the encrypted data object, the user identifier associated with the user of the second client device (*e.g.*, Microsoft server makes a selection of the identity provider automatically based on the email address of the authorized email recipient).[24]

57. On information and belief, the Accused Products with OME automatically request, by the access control management system (*e.g.*, Microsoft server), from the selected identity provider (*e.g.*, third-party service such as Google or Yahoo), authentication of the user of the second client device (*e.g.*, when the email recipient clicks "Sign in with Google" and provides his or her username and password, Microsoft server automatically requests identity authentication from Google)).[25]

58. On information and belief, the Accused Products with OME send, by the access control management system (*e.g.*, Microsoft server), to the second client device (*e.g.*, an email

[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*

recipient's device), the received information associated with the encrypted data object (*e.g.*, the metadata associated with the encrypted email), responsive to the authentication by the selected identity provider of the user of the second client device (*e.g.*, after the recipient successfully signs in, the Microsoft server sends the metadata associated with the encrypted email to the recipient).[26]

59. On information and belief, the Accused Products with OME receive, by the access control management system (*e.g.*, Microsoft server), from the first client device (*e.g.*, an email creator's device using Microsoft Office 365), information associated with a second encrypted data object (*e.g.*, the metadata associated with a second encrypted email).[27]

60. On information and belief, the Accused Products with OME receive, by the access control management system (*e.g.*, Microsoft server), from a third client device (*e.g.*, a second email recipient's device), a request for the information associated with the second encrypted data object (*e.g.*, a second recipient clicks "Read the message" button, thereby sending a request to the Microsoft server to access the metadata associated with the second encrypted email).[28]

61. On information and belief, the Accused Products with OME verify, by the access control management system (*e.g.*, Microsoft server), that a user of the third client device (*e.g.*, a second email recipient) is identified in the received information associated with the second encrypted data object (*e.g.*, Microsoft server verifies that the second email recipient's email is included in the metadata associated with the second encrypted email).[29]

62. On information and belief, the Accused Products with OME automatically select, by the access control management system (*e.g.*, Microsoft server), a second identity provider from the plurality of identity providers (*e.g.*, a second third-party service such as Google or Yahoo),

[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*

based on a second user identifier included in the received information associated with the second encrypted data object, the second user identifier associated with the user of the third client device (*e.g.*, Microsoft server makes a selection of the second identity provider automatically based on the email address of the second authorized email recipient).[30]

63. On information and belief, the Accused Products with OME automatically request, by the access control management system (*e.g.*, Microsoft server), from the selected second identity provider (*e.g.*, third-party service such as Google or Yahoo), authentication of the user of the third client device (*e.g.*, when the second email recipient clicks "Sign in with Google" and provides his or her username and password, Microsoft server automatically requests identity authentication from Google)).[31]

64. On information and belief, the Accused Products with OME send, to the third client device (*e.g.*, a second email recipient's device), the received information associated with the second encrypted data object (*e.g.*, the metadata associated with the second encrypted email), responsive to the authentication of the user of the third client device by the second identity provider (*e.g.*, after the second recipient successfully signs in, the Microsoft server sends the metadata associated with the second encrypted email to the second recipient).[32]

65. On information and belief, Microsoft has specifically intended, and continues to specifically intend, its customers to use the Accused Products with OME in a manner that infringes at least claim 1 of the '673 Patent. Microsoft has intentionally encouraged, instructed, and/or directed infringing use through training videos, demonstrations, brochures, user guides, and technical documentation.[33]

---

[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *See, e.g.*, *Message Policy and Compliance: Office 365 Message Encryption*, Microsoft (Apr. 8, 2021),

Infringement of Claim 1 of the '673 Patent by Accused Products with AP

66. Microsoft's AP feature is a service that allows users to securely share applications, services, and documents with authorized guest users, where authentication is performed by an identity provider (e.g., a third-party service such as Google) that is automatically selected based on information about the authorized guest users (e.g., the guest user's email address). The Accused Products with the AP feature employ the method of at least claim 1 of the '673 Patent for sharing secure information with authenticated recipients.

67. On information and belief, the Accused Products with AP practice a method for distributing cryptographic data to authenticated recipients via secured or unsecured channels. For example, on information and belief, the Accused Products with AP allow the sharing of a "company's applications and services with guest users from any other organization, while maintaining control over [its] own corporate data."[34]

68. On information and belief, the Accused Products with AP receive, by an access control management system (*e.g.*, Microsoft server), from a first client device (*e.g.*, a device of a user in an Azure tenant using Azure Portal and B2B) information associated with an encrypted data object (*e.g.*, a list of the users allowed to access a particular application where an encrypted data object resides and access permissions for the users).[35]

69. On information and belief, the Accused Products with AP receive, by the access

---

https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/message-policy-and-compliance?redirectedfrom=MSDN#bkmk_O365_MessageEncryption; Microsoft Ignite, *Protect and control your sensitive emails with new Office 365 Message Encryption capabilities*, YouTube (Sept. 28, 2017), https://www.youtube.com/watch?v=R3cDOFXToNQ&t=1087s.

[34] *What Is Guest User Access in Azure Active Directory B2B?*, Microsoft (Oct. 22, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b.

[35] Microsoft Mechanics, *Azure Active Directory B2B Collaboration: simple, secure external sharing of your Apps and Services*, YouTube (Apr. 12, 2017), https://youtu.be/AhwrweCBdsc?t=383; *Restrict guest access permissions in Azure Active Directory*, Microsoft (Dec. 29, 2021), https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-restrict-guest-permissions.

control management system (*e.g.*, Microsoft server), from a second client device (*e.g.*, a device of a guest user), a request for the information associated with the encrypted data object (*e.g.*, an invited guest user clicks on a redemption link in an invitation email, thereby sending a request to the Microsoft server to access the list of the users allowed to access the particular application where the encrypted data object resides and the access permissions for the users).[36]

70. On information and belief, the Accused Products with AP verify, by the access control management system (*e.g.*, Microsoft server), that a user of the second client device (*e.g.*, a guest user) is identified in the received information associated with the encrypted data object (*e.g.*, the Microsoft server verifies that the guest user was invited and is among the list of the users allowed to access the particular application where the encrypted data object resides).[37]

71. On information and belief, the Accused Products with AP automatically select, by the access control management system (*e.g.*, Microsoft server), an identity provider from a plurality of identity providers (*e.g.*, third-party service such as Google or another federated service), based on a user identifier included in the received information associated with the encrypted data object, the user identifier associated with the user of the second client device (*e.g.*, Microsoft server makes a selection of the identity provider automatically based on the email address of the authorized guest user).[38]

72. On information and belief, the Accused Products with AP automatically request, by the access control management system (*e.g.*, Microsoft server), from the selected identity provider (*e.g.*, third-party service such as Google or another federated service), authentication of

[36] *The elements of the B2B collaboration invitation email – Azure Active Directory*, Microsoft (Jul. 2, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/invitation-email-elements.
[37] *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133.
[38] *Id.*; *Azure Active Directory B2B collaboration invitation redemption*, Microsoft (Dec. 14, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/redemption-experience.

the user of the second client device (*e.g.*, when the guest user clicks on the redemption link and provides his or her username and password, Microsoft server automatically requests identity authentication from Google).[39]

73. On information and belief, the Accused Products with AP send, by the access control management system (*e.g.*, Microsoft server), to the second client device (*e.g.*, a guest user's device), the received information associated with the encrypted data object, responsive to the authentication by the selected identity provider of the user of the second client device (*e.g.*, after the recipient successfully signs in, the guest user can access the list of the users allowed to access the particular application where the encrypted data object resides and the access permissions for the users).[40]

74. On information and belief, the Accused Products with AP receive, by the access control management system (*e.g.*, Microsoft server), from a first client device (*e.g.*, a device of a user in an Azure tenant using Azure Portal and B2B) information associated with a second encrypted data object (*e.g.*, a list of the users allowed to access a particular application where a second encrypted data object resides and the access permissions for the users).[41]

75. On information and belief, the Accused Products with AP receive, by the access control management system (*e.g.*, Microsoft server), from a third client device (*e.g.*, a device of a second guest user), a request for the information associated with the second encrypted data object

[39] *Id.*; *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133; Microsoft Security, *Manage partner access with Azure AD B2B collaboration*, YouTube (Aug. 20, 2020), https://youtu.be/AO-uTWSmU_E?t=308.
[40] *See, e.g.*, *What are the default user permissions in Azure Active Directory?*, Microsoft (Dec. 22, 2021), https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions.
[41] Microsoft Mechanics, *Azure Active Directory B2B Collaboration: simple, secure external sharing of your Apps and Services*, YouTube (Apr. 12, 2017), https://youtu.be/AhwrweCBdsc?t=383; *Restrict guest access permissions in Azure Active Directory*, Microsoft (Dec. 29, 2021), https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-restrict-guest-permissions.

(*e.g.*, a second invited guest user clicks on a redemption link in an invitation email, thereby sending a request to the Microsoft server to access the list of the users allowed to access a particular application where the second encrypted data object resides and the access permissions for the users).[42]

76. On information and belief, the Accused Products with AP verify, by the access control management system (*e.g.*, Microsoft server), that a user of the third client device (*e.g.*, a second guest user) is identified in the received information associated with the second encrypted data object (*e.g.*, the Microsoft server verifies that the second guest user was invited and is among the list of the users allowed to access a particular application where the second encrypted data object resides).[43]

77. On information and belief, the Accused Products with AP automatically select, by the access control management system (*e.g.*, Microsoft server), a second identity provider from a plurality of identity providers (*e.g.*, third-party service such as Google or another federated service), based on a user identifier included in the received information associated with the second encrypted data object, the user identifier associated with the user of the third client device (*e.g.*, Microsoft server makes a selection of the identity provider automatically based on the email address of the second authorized guest user).[44]

78. On information and belief, the Accused Products with AP automatically request, by the access control management system (*e.g.*, Microsoft server), from the selected second identity provider (*e.g.*, third-party service such as Google or another federated service),

[42] *The elements of the B2B collaboration invitation email – Azure Active Directory*, Microsoft (Jul. 2, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/invitation-email-elements.
[43] *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133.
[44] *Id.*; *Azure Active Directory B2B collaboration invitation redemption*, Microsoft (Dec. 14, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/redemption-experience.

authentication of the user of the third client device (*e.g.*, when the second guest user clicks on a redemption link and provides his or her username and password, Microsoft server automatically requests identity authentication from Google).[45]

79. On information and belief, the Accused Products with AP send, by the access control management system (*e.g.*, Microsoft server), to the third client device (*e.g.*, a second guest user's device), the received information associated with the second encrypted data object, responsive to the authentication of the user of the third client device by the second identity provider (*e.g.*, after the second guest user successfully signs in, the second guest user can access the list of the users allowed to access the particular application where the second encrypted data object resides and the access permissions for the users).[46]

80. On information and belief, Microsoft has specifically intended, and continues to specifically intend, its customers to use the Accused Products with AP in a manner that infringes at least claim 1 of the '673 Patent. Microsoft has intentionally encouraged, instructed, and/or directed infringing use through training videos, demonstrations, brochures, user guides, and technical documentation.[47]

Infringement of Claim 1 of the '673 Patent by Accused Products with AKV

81. Microsoft's AKV feature is a service that allows users to share cryptographic keys that are used to encrypt files with authorized guest users, where authentication is performed by an

[45] *Id.*; *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133; Microsoft Security, *Manage partner access with Azure AD B2B collaboration*, YouTube (Aug. 20, 2020), https://youtu.be/AO-uTWSmU_E?t=308.
[46] *See, e.g.*, *What are the default user permissions in Azure Active Directory?*, Microsoft (Dec. 22, 2021), https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions.
[47] *See, e.g.*, *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133; Microsoft Security, *Manage partner access with Azure AD B2B collaboration*, YouTube (Aug. 20, 2020), https://youtu.be/AO-uTWSmU_E?t=308.

identity provider (e.g., a third-party service such as Google) that is automatically selected based on information about the authorized guest users (e.g., the guest user's email address). The Accused Products with the AKV feature employ the method of at least claim 1 of the '673 Patent for sharing secure information with authenticated recipients.

82. The Accused Products with AKV employ a method for sharing secure information with authenticated recipients, in which the authentication is performed by an identity provider that is automatically selected based on the secure information.

83. On information and belief, the Accused Products with AKV practice a method for distributing cryptographic data to authenticated recipients via secured or unsecured channels. For example, on information and belief, the Accused Products with AKV allow the sharing of "keys, secrets, and certificates stored in [Azure Key Vault]" with "users both within an organization and outside."[48]

84. On information and belief, the Accused Products with AKV receive, by an access control management system (*e.g.*, Microsoft server), from a first client device (*e.g.*, a device of a user in an Azure tenant using Azure Key Vault and B2B) information associated with an encrypted data object (*e.g.*, a cryptographic key that is used to encrypt an encrypted data object, a list of the users allowed to access the Azure Key Vault where the cryptographic key resides, and access permissions for the users).[49]

85. On information and belief, the Accused Products with AKV receive, by the access

[48] *Secure Your Sensitive Business Information with Azure Key Vault*, Microsoft (Jan. 4, 2019), https://docs.microsoft.com/en-us/archive/msdn-magazine/2018/march/azure-secure-your-sensitive-business-information-with-azure-key-vault.

[49] *Assign a Key Vault access policy*, Microsoft (Sep. 10, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal; *Provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control*, Microsoft (Oct. 16, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli; Microsoft Security, Azure Key Vault: What's new, YouTube (Sep. 22, 2020), https://youtu.be/d8Xv6PJEfPw?t=137.

control management system (*e.g.*, Microsoft server), from a second client device (*e.g.*, a device of a guest user), a request for the information associated with the encrypted data object (*e.g.*, an invited guest user clicks on a redemption link in an invitation email, thereby sending a request to the Microsoft server to access the cryptographic key that is used to encrypt the encrypted data object, the list of the users allowed to access the Azure Key Vault where the cryptographic key resides, and the access permissions for the users)[50].

86. On information and belief, the Accused Products with AKV verify, by the access control management system (*e.g.*, Microsoft server), that a user of the second client device (*e.g.*, a guest user) is identified in the received information associated with the encrypted data object (*e.g.*, the Microsoft server verifies that the guest user was invited and is among the list of the users allowed to access the Azure Key Vault where the cryptographic key that is used to encrypt the encrypted data object resides).[51]

87. On information and belief, the Accused Products with AKV automatically select, by the access control management system (*e.g.*, Microsoft server), an identity provider from a plurality of identity providers (*e.g.*, third-party service such as Google or another federated service), based on a user identifier included in the received information associated with the encrypted data object, the user identifier associated with the user of the second client device (*e.g.*, Microsoft server makes a selection of the identity provider automatically based on the email address of the authorized guest user).[52]

88. On information and belief, the Accused Products with AKV automatically request,

---

[50] *The elements of the B2B collaboration invitation email – Azure Active Directory*, Microsoft (Jul. 2, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/invitation-email-elements.
[51] *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133.
[52] *Id.*; *Azure Active Directory B2B collaboration invitation redemption*, Microsoft (Dec. 14, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/redemption-experience.

by the access control management system (*e.g.*, Microsoft server), from the selected identity provider (*e.g.*, third-party service such as Google or another federated service), authentication of the user of the second client device (*e.g.*, when the guest user clicks on a redemption link and provides his or her username and password, Microsoft server automatically requests identity authentication from Google)).[53]

89. On information and belief, the Accused Products with AKV send, by the access control management system (*e.g.*, Microsoft server), to the second client device (*e.g.*, a guest user's device), the received information associated with the encrypted data object, responsive to the authentication by the selected identity provider of the user of the second client device (*e.g.*, after the guest user successfully signs in, the guest user can access the cryptographic key that is used to encrypt the encrypted data object, the list of the users allowed to access the Azure Key Vault where the cryptographic key resides, and the access permissions for the users)[54].

90. On information and belief, the Accused Products with AKV receive, by the access control management system (e.g., Microsoft server), from a first client device (*e.g.*, a device of a user in an Azure tenant using Azure Key Vault and B2B) information associated with a second encrypted data object (*e.g.*, a cryptographic key that is used to encrypt another encrypted data object, a list of the users allowed to access the Azure Key Vault where the cryptographic key resides, and access permissions for the users).[55]

---

[53] *Id.*; *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133; Microsoft Security, *Manage partner access with Azure AD B2B collaboration*, YouTube (Aug. 20, 2020), https://youtu.be/AO-uTWSmU_E?t=308.

[54] *See, e.g.*, *Azure Key Vault security*, Microsoft (Dec. 9, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/security-features.

[55] *Assign a Key Vault access policy*, Microsoft (Sep. 10, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal; *Provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control*, Microsoft (Oct. 16, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli; Microsoft Security, Azure Key Vault: What's new, YouTube (Sep. 22, 2020), https://youtu.be/d8Xv6PJEfPw?t=137.

91. On information and belief, the Accused Products with AKV receive, by the access control management system (*e.g.*, Microsoft server), from a third client device (*e.g.*, a device of a second guest user), a request for the information associated with the second encrypted data object (*e.g.*, an invited second guest user clicks on a redemption link, thereby sending a request to the Microsoft server to access the cryptographic key that is used to encrypt the second encrypted data object, the list of the users allowed to access the Azure Key Vault where the cryptographic key resides, and access permissions for the users).

92. On information and belief, the Accused Products with AKV verify, by the access control management system (*e.g.*, Microsoft server), that a user of the third client device (*e.g.*, a second guest user) is identified in the received information associated with the second encrypted data object (*e.g.*, the Microsoft server verifies that the second guest user was invited and is among the list of the users allowed to access the Azure Key Vault where the cryptographic key that is used to encrypt the second encrypted data object resides).[56]

93. On information and belief, the Accused Products with AKV automatically select, by the access control management system (*e.g.*, Microsoft server), a second identity provider from a plurality of identity providers (*e.g.*, third-party service such as Google or another federated service), based on a second user identifier included in the received information associated with the second encrypted data object, the second user identifier associated with the user of the third client device (*e.g.*, Microsoft server makes a selection of the second identity provider automatically based on the email address of the second authorized guest user).[57]

94. On information and belief, the Accused Products with AKV automatically request,

[56] *The elements of the B2B collaboration invitation email – Azure Active Directory*, Microsoft (Jul. 2, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/invitation-email-elements.
[57] *Id.*; *Azure Active Directory B2B collaboration invitation redemption*, Microsoft (Dec. 14, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/redemption-experience.

by the access control management system (*e.g.*, Microsoft server), from the selected second identity provider (*e.g.*, third-party service such as Google or another federated service), authentication of the user of the third client device (*e.g.*, when the second guest user clicks on a redemption link and provides his or her username and password, Microsoft server automatically requests identity authentication from Google)).[58]

95. On information and belief, the Accused Products with AKV send, by the access control management system (*e.g.*, Microsoft server), to the third client device (*e.g.*, a second guest user's device), the received information associated with the second encrypted data object, responsive to the authentication by the selected second identity provider of the user of the third client device (*e.g.*, after the second guest user successfully signs in, the second guest user can access the cryptographic key that is used to encrypt the second encrypted data object, the list of the users allowed to access the Azure Key Vault where the cryptographic key resides, and the access permissions for the users).[59]

96. On information and belief, Microsoft has specifically intended, and continues to specifically intend, its customers to use the Accused Products with AKV in a manner that infringes at least claim 1 of the '673 Patent. Microsoft has intentionally encouraged, instructed, and/or directed infringing use through training videos, demonstrations, brochures, user guides, and technical documentation.[60]

---

[58] *Id.*; *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133; Microsoft Security, *Manage partner access with Azure AD B2B collaboration*, YouTube (Aug. 20, 2020), https://youtu.be/AO-uTWSmU_E?t=308.

[59] *See, e.g.*, *Azure Key Vault security*, Microsoft (Dec. 9, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/security-features.

[60] *Secure Your Sensitive Business Information with Azure Key Vault*, Microsoft (Jan. 4, 2019), https://docs.microsoft.com/en-us/archive/msdn-magazine/2018/march/azure-secure-your-sensitive-business-information-with-azure-key-vault; *Assign a Key Vault access policy*, Microsoft (Sep. 10, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal.

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 8,874,902

97. Virtru incorporates herein by reference the allegations stated above in paragraphs 1–96 of this Complaint.

98. On information and belief, Microsoft has been and is now directly infringing the '902 Patent in this district and elsewhere, in violation of 35 U.S.C. § 271(a) at least by making, using, selling, offering for sale, and/or importing into the United States, Accused Products that practice one or more claims of the '902 Patent, including at least claims 1 and 3.

99. Microsoft has committed infringing acts without the permission, consent, authorization, or license of Virtru.

100. Microsoft's infringement is literal, under the doctrine of equivalents, or both.

101. On information and belief, Microsoft has been and is now indirectly infringing the '902 Patent in violation of 35 U.S.C. § 271(b) at least by inducing its customers to purchase the Accused Products and/or by instructing, encouraging, and/or directing others how to use the Accused Products in ways that directly infringe at least claims 1 and 3 of the '902 Patent.

102. On information and belief, by using the Accused Products as encouraged and directed by Microsoft, Microsoft's customers directly infringe one or more claims of the '902 Patent, including at least claims 1 and 3. For example, through its product manuals, sales and marketing activities, support activities, and other materials and activities, Microsoft solicits, instructs, encourages, and aids and abets its customers to purchase and use the Accused Products in infringing ways.[61]

[61] *See, e.g.*, *Message Policy and Compliance: Office 365 Message Encryption*, Microsoft (Apr. 8, 2021), https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/message-policy-and-compliance?redirectedfrom=MSDN#bkmk_O365_MessageEncryption; Microsoft Ignite, *Protect and control your sensitive emails with new Office 365 Message Encryption capabilities*, YouTube (Sept. 28, 2017),

103. Microsoft has had knowledge of the '902 Patent and its infringement of the '902 Patent since at least service of this Complaint.

104. Furthermore, on information and belief, Microsoft knew or was at least willfully blind to the existence of the '902 Patent and its infringement of the '902 Patent.

105. These facts give rise to a reasonable inference that Microsoft has knowingly induced its customers to infringe at least claims 1 and 3 of the '902 Patent directly, and that Microsoft has possessed a specific intent to cause such direct infringement. Further discovery may reveal earlier or additional knowledge of the '902 Patent, which would provide additional evidence of Microsoft's intent to induce infringement.

106. Microsoft's infringement of the '902 Patent has been and continues to be deliberate and willful, and this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees and costs pursuant to 35 U.S.C. §§ 284 and 285.

107. On information and belief, Microsoft lacks a good faith belief that the claims of the '902 Patent Suit are not infringed, invalid, or unenforceable.

108. On information and belief, Microsoft will continue to infringe the '902 Patent, causing irreparable harm for which there is no adequate remedy at law, unless enjoined by this Court. On information and belief, Microsoft's infringement of the '902 Patent has caused and continues to cause irreparable harm to Virtru, including in this district, in the form of, among other things, loss of market share; price erosion; lost business opportunities and sales; loss of goodwill associated with Virtru's innovative technologies; entry into the market of additional infringers; and loss of its exclusive right to license its invention.

109. Because of Microsoft's infringement of the '902 Patent, Virtru has suffered and is

https://www.youtube.com/watch?v=R3cDOFXToNQ&t=1087s; .

owed monetary damages adequate to compensate it for the infringement under 35 U.S.C. § 284, but in no event less than a reasonable royalty.

110. Microsoft and its customers infringe at least claims 1 and 3 of the '902 Patent as set forth below.[62]

Infringement of Claim 3 of '902 Patent by Accused Products with OME

111. Claim 3 of the '902 Patent discloses a method for sharing secure information with authenticated recipients, in which the authentication is performed by an identity provider that is selected based on information about the authorized recipients, and when the secure information is only accessible to the authenticated recipients within a designated time period.

112. The Accused Products with OME employ the method of at least claim 3 of the '902 Patent for sharing secure information with authenticated recipients.

113. On information and belief, the Accused Products with OME practice a method for distributing cryptographic data to authenticated recipients via secured or unsecured channels. For example, on information and belief, the Accused Products with OME "allow[] email users to send encrypted email messages to anyone," which "provide enhanced end user experiences that make it easier to share and collaborate on protected messages with anyone inside or outside the organization."[63]

114. On information and belief, the Accused Products with OME receive, by an access control management system (*e.g.*, Microsoft server), from a first client device (*e.g.*, an email creator's device using Microsoft Office 365), information associated with an encrypted data object

[62] Certain claim language in the '902 patent was corrected through a certificate of correction issued by the USPTO on February 15, 2022.

[63] *Message Policy and Compliance: Office 365 Message Encryption*, Microsoft (Apr. 8, 2021), https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/message-policy-and-compliance?redirectedfrom=MSDN#bkmk_O365_MessageEncryption.

(*e.g.*, the metadata associated with the encrypted email), the information including a specification that a user may receive the information within a time period (*e.g.*, an expiration date for the email, after which the email can no longer be accessed).[64]

115. On information and belief, the Accused Products with OME receive, by the access control management system (*e.g.*, Microsoft server), from a second client device (*e.g.*, an email recipient's device), a request for the information associated with the encrypted data object (*e.g.*, a recipient clicks "Read the message" button, thereby sending a request to the Microsoft server to access the metadata associated with the encrypted email).[65]

116. On information and belief, the Accused Products with OME verify, by the access control management system (*e.g.*, Microsoft server), that a user of the second client device (*e.g.*, an email recipient) is identified in the received information associated with the encrypted data object (*e.g.*, Microsoft server verifies that the email recipient's email is included in the metadata associated with the encrypted email).[66]

117. On information and belief, the Accused Products with OME select, by the access control management system (*e.g.*, Microsoft server), an identity provider from a plurality of identity providers (*e.g.*, third-party service such as Google or Yahoo), based on a user identifier included in the received information associated with the encrypted data object, the user identifier associated with the user of the second client device (*e.g.*, Microsoft server makes a selection of the identity provider based on the email address of the authorized email recipient).[67]

118. On information and belief, the Accused Products with OME request, by the access

---

[64] Microsoft Ignite, *Protect and control your sensitive emails with new Office 365 Message Encryption capabilities*, YouTube (Sept. 28, 2017), https://www.youtube.com/watch?v=R3cDOFXToNQ&t=1087s; *Set an expiration date for email encrypted by Office 365 Advanced Message Encryption*, Microsoft (Oct. 5, 2021), https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-advanced-expiration?view=o365-worldwide.
[65] *Id.*
[66] *Id.*
[67] *Id.*

control management system (*e.g.*, Microsoft server), from the selected identity provider (*e.g.*, third-party service such as Google or Yahoo), authentication of the user of the second client device (*e.g.*, when the email recipient clicks "Sign in with Google" and provides his or her username and password, Microsoft server requests identity authentication from Google).[68]

119. On information and belief, the Accused Products with OME send, by the access control management system (*e.g.*, Microsoft server), to the second client device (*e.g.*, an email recipient's device), the received information associated with the encrypted data object (*e.g.*, the metadata associated with encrypted email), responsive to the authentication by the selected identity provider of the user of the second client device (*e.g.*, after the recipient successfully signs in, the Microsoft server sends the metadata associated with the encrypted email to the recipient).[69]

120. On information and belief, Microsoft has specifically intended, and continues to specifically intend, its customers to use the Accused Products with OME in a manner that infringes at least claim 3 of the '902 Patent. Microsoft has intentionally encouraged, instructed, and/or directed infringing use through training videos, demonstrations, brochures, user guides, and technical documentation.[70]

Infringement of Claim 1 of '902 Patent by Accused Products with AP

121. Claim 1 of the '902 Patent discloses a method for sharing secure information with authenticated recipients, in which the authentication is performed by an identity provider that is selected based on information about the authorized recipients, and when the authorized recipients

[68] *Id.*
[69] *Id.*
[70] *See, e.g.*, *Message Policy and Compliance: Office 365 Message Encryption*, Microsoft (Apr. 8, 2021), https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/message-policy-and-compliance?redirectedfrom=MSDN#bkmk_O365_MessageEncryption; Microsoft Ignite, *Protect and control your sensitive emails with new Office 365 Message Encryption capabilities*, YouTube (Sept. 28, 2017), https://www.youtube.com/watch?v=R3cDOFXToNQ&t=1087s; *Set an expiration date for email encrypted by Office 365 Advanced Message Encryption*, Microsoft (Oct. 5, 2021), https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-advanced-expiration?view=o365-worldwide.

are assigned roles.

122. The Accused Products with AP employ the method of at least claim 1 of the '902 Patent for sharing secure information with authenticated recipients.

123. On information and belief, the Accused Products with AP practice a method for distributing cryptographic data to authenticated recipients via secured or unsecured channels. For example, on information and belief, the Accused Products with AP allow the sharing of a "company's applications and services with guest users from any other organization, while maintaining control over [its] own corporate data."[71]

124. On information and belief, the Accused Products with AP receive, by an access control management system (*e.g.*, Microsoft server), from a first client device (*e.g.*, a device of a user in an Azure tenant using Azure Portal and B2B) information associated with an encrypted data object (*e.g.*, a list of the users allowed to access a particular application where an encrypted data object resides and access permissions for the users), the information including an identification of a role assigned to a user authorized to access the encrypted data object (*e.g.*, a user in an Azure tenant can enter a collection of permissions either built in or customized that are supported by Azure Active Directory role-based access control (Azure RBAC) for other users).[72]

125. On information and belief, the Accused Products with AP receive, by the access control management system (*e.g.*, Microsoft server), from a second client device (*e.g.*, a device of a guest user), a request for the information associated with the encrypted data object (*e.g.*, an

[71] *What Is Guest User Access in Azure Active Directory B2B?*, Microsoft (Oct. 22, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b.

[72] Microsoft Mechanics, *Azure Active Directory B2B Collaboration: simple, secure external sharing of your Apps and Services*, YouTube (Apr. 12, 2017), https://youtu.be/AhwrweCBdsc?t=383; *Restrict guest access permissions in Azure Active Directory*, Microsoft (Dec. 29, 2021), https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-restrict-guest-permissions; *What is Azure role-based access control (Azure RBAC)?*, Microsoft (Dec. 29, 2021), https://docs.microsoft.com/en-us/azure/role-based-access-control/overview; *Assign Azure roles to external guest users using the Azure portal*, Microsoft (Dec. 29, 2021), https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-external-users.

invited guest user clicks on a redemption link in an invitation email, thereby sending a request to the Microsoft server to access the list of the users allowed to access the particular application where the encrypted data object resides and the access permissions for the users).[73]

126. On information and belief, the Accused Products with AP verify, by the access control management system (*e.g.*, Microsoft server), that a user of the second client device (*e.g.*, a guest user) is identified in the received information associated with the encrypted data object (*e.g.*, the Microsoft server verifies that the guest user was invited and is among the list of the users allowed to access the particular application where the encrypted data object resides).[74]

127. On information and belief, the Accused Products with AP verify, by the access control management system (*e.g.*, Microsoft server), that the user of the second client device (*e.g.*, a guest user) is assigned the role identified in the received information (*e.g.*, Microsoft server evaluates the guest user's role memberships based on the guest user's access token).[75]

128. On information and belief, the Accused Products with AP select, by the access control management system (*e.g.*, Microsoft server), an identity provider from a plurality of identity providers (*e.g.*, third-party service such as Google or another federated service), based on a user identifier included in the received information associated with the encrypted data object, the user identifier associated with the user of the second client device (*e.g.*, Microsoft server makes a selection of the identity provider based on the email address of the authorized guest user).[76]

129. On information and belief, the Accused Products with AP request, by the access

[73] *The elements of the B2B collaboration invitation email – Azure Active Directory*, Microsoft (Jul. 2, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/invitation-email-elements.
[74] *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133.
[75] *Overview of role-based access control in Azure Active Directory*, Microsoft (Dec. 29, 2021), https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-overview.
[76] *Id.*; *Azure Active Directory B2B collaboration invitation redemption*, Microsoft (Dec. 14, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/redemption-experience.

control management system (*e.g.*, Microsoft server), from the selected identity provider (*e.g.*, third-party service such as Google or another federated service), authentication of the user of the second client device (*e.g.*, when the guest user clicks on the redemption link and provides his or her username and password, Microsoft server requests identity authentication from Google).[77]

130. On information and belief, the Accused Products with AP send, by the access control management system (*e.g.*, Microsoft server), to the second client device (*e.g.*, a guest user's device), the received information associated with the encrypted data object, responsive to the authentication by the selected identity provider of the user of the second client device (*e.g.*, after the recipient successfully signs in, the guest user can access the list of the users allowed to access the particular application where the encrypted data object resides and the access permissions for the users).[78]

131. On information and belief, Microsoft has specifically intended, and continues to specifically intend, its customers to use the Accused Products with AP in a manner that infringes at least claim 1 of the '902 Patent. Microsoft has intentionally encouraged, instructed, and/or directed infringing use through training videos, demonstrations, brochures, user guides, and technical documentation.[79]

Infringement of Claim 1 of '902 Patent by Accused Products with AKV

132. The Accused Products with AKV employ the method of at least claim 1 of the '902

[77] *Id.*; *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133; Microsoft Security, *Manage partner access with Azure AD B2B collaboration*, YouTube (Aug. 20, 2020), https://youtu.be/AO-uTWSmU_E?t=308.
[78] *See, e.g.*, *What are the default user permissions in Azure Active Directory?*, Microsoft (Dec. 22, 2021), https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions.
[79] *See, e.g.*, *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133; Microsoft Security, *Manage partner access with Azure AD B2B collaboration*, YouTube (Aug. 20, 2020), https://youtu.be/AO-uTWSmU_E?t=308; *Assign Azure roles to external guest users using the Azure portal*, Microsoft (Dec. 29, 2021), https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-external-users.

Patent for sharing secure information with authenticated recipients, in which the authentication is performed by an identity provider that is selected based on information about the authorized recipients, and when the authorized recipients are assigned roles.

133. On information and belief, the Accused Products with AKV practice a method for distributing cryptographic data to authenticated recipients via secured or unsecured channels. For example, on information and belief, the Accused Products with AKV allow the sharing of "keys, secrets, and certificates stored in [Azure Key Vault]" with "users both within an organization and outside."[80]

134. On information and belief, the Accused Products with AKV receive, by an access control management system (*e.g.*, Microsoft server), from a first client device (*e.g.*, a device of a user in an Azure tenant using Azure Key Vault and B2B) information associated with an encrypted data object (*e.g.*, a cryptographic key that is used to encrypt an encrypted data object, a list of the users allowed to access the Azure Key Vault where the cryptographic key resides, and access permissions for the users), the information including an identification of a role assigned to a user authorized to access the encrypted data object (*e.g.*, a user in an Azure tenant can enter a collection of permissions either built in or customized that are supported by Azure Active Directory role-based access control (Azure RBAC) for other users).[81]

135. On information and belief, the Accused Products with AKV receive, by the access control management system (*e.g.*, Microsoft server), from a second client device (*e.g.*, a device of

[80] *Secure Your Sensitive Business Information with Azure Key Vault*, Microsoft (Jan. 4, 2019), https://docs.microsoft.com/en-us/archive/msdn-magazine/2018/march/azure-secure-your-sensitive-business-information-with-azure-key-vault.

[81] *Assign a Key Vault access policy*, Microsoft (Sep. 10, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal; *Provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control*, Microsoft (Oct. 16, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli; Microsoft Security, Azure Key Vault: What's new, YouTube (Sep. 22, 2020), https://youtu.be/d8Xv6PJEfPw?t=137; *What is Azure role-based access control (Azure RBAC)?*, Microsoft (Dec. 29, 2021), https://docs.microsoft.com/en-us/azure/role-based-access-control/overview.

a guest user), a request for the information associated with the encrypted data object (*e.g.*, an invited guest user clicks on a redemption link in an invitation email, thereby sending a request to the Microsoft server to access the cryptographic key that is used to encrypt the encrypted data object, the list of the users allowed to access the Azure Key Vault where the cryptographic key resides, and the access permissions for the users)[82].

136. On information and belief, the Accused Products with AKV verify, by the access control management system (*e.g.*, Microsoft server), that a user of the second client device (*e.g.*, a guest user) is identified in the received information associated with the encrypted data object (*e.g.*, the Microsoft server verifies that the guest user was invited and is among the list of the users allowed to access the Azure Key Vault where the cryptographic key that is used to encrypt the encrypted data object resides).[83]

137. On information and belief, the Accused Products with AKV verify, by the access control management system (*e.g.*, Microsoft server), that the user of the second client device (*e.g.*, a guest user) is assigned the role identified in the received information (*e.g.*, Microsoft server evaluates the guest user's role memberships based on the guest user's access token).[84]

138. On information and belief, the Accused Products with AKV select, by the access control management system (*e.g.*, Microsoft server), an identity provider from a plurality of identity providers (*e.g.*, third-party service such as Google or another federated service), based on a user identifier included in the received information associated with the encrypted data object, the user identifier associated with the user of the second client device (*e.g.*, Microsoft server makes

[82] *The elements of the B2B collaboration invitation email – Azure Active Directory*, Microsoft (Jul. 2, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/invitation-email-elements.
[83] *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133.
[84] *Overview of role-based access control in Azure Active Directory*, Microsoft (Dec. 29, 2021), https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-overview.

a selection of the identity provider based on the email address of the authorized guest user).[85]

139. On information and belief, the Accused Products with AKV request, by the access control management system (*e.g.*, Microsoft server), from the selected identity provider (*e.g.*, third-party service such as Google or another federated service), authentication of the user of the second client device (*e.g.*, when the guest user clicks on a redemption link and provides his or her username and password, Microsoft server requests identity authentication from Google)).[86]

140. On information and belief, the Accused Products with AKV send, by the access control management system (*e.g.*, Microsoft server), to the second client device (*e.g.*, a guest user's device), the received information associated with the encrypted data object, responsive to the authentication by the selected identity provider of the user of the second client device (*e.g.*, after the guest user successfully signs in, the guest user can access the cryptographic key that is used to encrypt the encrypted data object, the list of the users allowed to access the Azure Key Vault where the cryptographic key resides, and the access permissions for the users).[87]

141. On information and belief, Microsoft has specifically intended, and continues to specifically intend, its customers to use the Accused Products with AKV in a manner that infringes at least claim 1 of the '902 Patent. Microsoft has intentionally encouraged, instructed, and/or directed infringing use through training videos, demonstrations, brochures, user guides, and technical documentation.[88]

---

[85] *Id.*; *Azure Active Directory B2B collaboration invitation redemption*, Microsoft (Dec. 14, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/redemption-experience.

[86] *Id.*; *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133; Microsoft Security, *Manage partner access with Azure AD B2B collaboration*, YouTube (Aug. 20, 2020), https://youtu.be/AO-uTWSmU_E?t=308.

[87] *See, e.g.*, *Azure Key Vault security*, Microsoft (Dec. 9, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/security-features.

[88] *Secure Your Sensitive Business Information with Azure Key Vault*, Microsoft (Jan. 4, 2019), https://docs.microsoft.com/en-us/archive/msdn-magazine/2018/march/azure-secure-your-sensitive-business-information-with-azure-key-vault; *Assign a Key Vault access policy*, Microsoft (Sep. 10, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal; *Provide access to*

COUNT III

INFRINGEMENT OF U.S. PATENT NO. 9,578,021

142. Virtru incorporates herein by reference the allegations stated above in paragraphs 1–141 of this Complaint.

143. On information and belief, Microsoft has been and is now directly infringing the '021 Patent in this district and elsewhere, in violation of 35 U.S.C. § 271(a) at least by making, using, selling, offering for sale, and/or importing into the United States, Accused Products that practice one or more claims of the '021 Patent, including at least claim 1.

144. Microsoft has committed infringing acts without the permission, consent, authorization, or license of Virtru.

145. Microsoft's infringement is literal, under the doctrine of equivalents, or both.

146. On information and belief, Microsoft has been and is now indirectly infringing the '021 Patent in violation of 35 U.S.C. § 271(b) at least by inducing its customers to purchase the Accused Products and/or by instructing, encouraging, and/or directing others how to use the Accused Products in ways that directly infringe at least claim 1 of the '021 Patent.

147. On information and belief, by using the Accused Products as encouraged and directed by Microsoft, Microsoft's customers directly infringe one or more claims of the '021 Patent, including at least claim 1. For example, through its product manuals, sales and marketing activities, support activities, and other materials and activities, Microsoft solicits, instructs, encourages, and aids and abets its customers to purchase and use the Accused Products in infringing ways.[89]

Key Vault keys, certificates, and secrets with an Azure role-based access control, Microsoft (Oct. 16, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli.

[89] *See, e.g.*, *Message Policy and Compliance: Office 365 Message Encryption*, Microsoft (Apr. 8, 2021), https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/message-

148. Microsoft has had knowledge of the '021 Patent since at least service of this Complaint.

149. Furthermore, on information and belief, Microsoft knew or was at least willfully blind to the existence of the '021 Patent and its infringement of the '021 Patent.

150. These facts give rise to a reasonable inference that Microsoft has knowingly induced its customers to infringe at least claim 1 of the '021 Patent directly, and that Microsoft has possessed a specific intent to cause such direct infringement. Further discovery may reveal earlier or additional knowledge of the '021 Patent, which would provide additional evidence of Microsoft's intent to induce infringement.

151. Microsoft's infringement of the '021 Patent has been and continues to be deliberate and willful, and this is therefore an exceptional case warranting an award of enhanced damages and attorneys' fees and costs pursuant to 35 U.S.C. §§ 284 and 285.

152. On information and belief, Microsoft lacks a good faith belief that the claims of the '021 Patent Suit are not infringed, invalid, or unenforceable.

153. On information and belief, Microsoft will continue to infringe the '021 Patent, causing irreparable harm for which there is no adequate remedy at law, unless enjoined by this Court. On information and belief, Microsoft's infringement of the '021 Patent has caused and continues to cause irreparable harm to Virtru, including in this district, in the form of, among other things, loss of market share; price erosion; lost business opportunities and sales; loss of goodwill associated with Virtru's innovative technologies; entry into the market of additional infringers; and loss of its exclusive right to license its invention.

---

policy-and-compliance?redirectedfrom=MSDN#bkmk_O365_MessageEncryption; Microsoft Ignite, *Protect and control your sensitive emails with new Office 365 Message Encryption capabilities*, YouTube (Sept. 28, 2017), https://www.youtube.com/watch?v=R3cDOFXToNQ&t=1087s.

154. As a result of Microsoft's infringement of the '021 Patent, Virtru has suffered and is owed monetary damages adequate to compensate it for the infringement under 35 U.S.C. § 284, but in no event less than a reasonable royalty.

155. Microsoft and its customers infringe at least claim 1 of the '021 Patent as set forth below.

Infringement of Claim 1 of '021 Patent by Accused Products with OME

156. Claim 1 of the '021 Patent discloses a method for sharing secure information with authenticated recipients, in which the authentication is performed by an identity provider that is automatically selected based on information about the authorized recipients, and when information about the authenticated recipients is stored in a transaction log.

157. The Accused Products with OME employ the method of at least claim 1 of the '021 Patent for sharing secure information with authenticated recipients.

158. On information and belief, the Accused Products with OME practice a method for distributing cryptographic data to trusted recipients. For example, on information and belief, the Accused Products with OME "allow[] email users to send encrypted email messages to anyone," which "provide enhanced end user experiences that make it easier to share and collaborate on protected messages with anyone inside or outside the organization."[90]

159. On information and belief, the Accused Products with OME receive, by an access control management system (*e.g.*, Microsoft server), from a first client device (*e.g.*, an email creator's device using Microsoft Office 365), information associated with an encrypted data object (*e.g.*, the metadata associated with encrypted email).[91]

[90] *Message Policy and Compliance: Office 365 Message Encryption*, Microsoft (Apr. 8, 2021), https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/message-policy-and-compliance?redirectedfrom=MSDN#bkmk_O365_MessageEncryption.

[91] Microsoft Ignite, *Protect and control your sensitive emails with new Office 365 Message Encryption capabilities*,

160. On information and belief, the Accused Products with OME receive, by the access control management system (*e.g.*, Microsoft server), from a second client device (*e.g.*, an email recipient's device), a request for the information associated with the encrypted data object (*e.g.*, a recipient clicks "Read the message" button, thereby sending a request to the Microsoft server to access the metadata associated with the encrypted email).[92]

161. On information and belief, the Accused Products with OME verify, by the access control management system (*e.g.*, Microsoft server), that a user of the second client device (*e.g.*, an email recipient) is identified in the received information associated with the encrypted data object (*e.g.*, Microsoft server verifies that the email recipient's email is included in the metadata associated with the encrypted email).[93]

162. On information and belief, the Accused Products with OME automatically select, by the access control management system (*e.g.*, Microsoft server), an identity provider from a plurality of identity providers (*e.g.*, third-party service such as Google or Yahoo), based on a user identifier included in the received information associated with the encrypted data object, the user identifier associated with the user of the second client device (*e.g.*, Microsoft server makes a selection of the identity provider automatically based on the email address of the authorized email recipient).[94]

163. On information and belief, the Accused Products with OME automatically request, by the access control management system (*e.g.*, Microsoft server), from the selected identity provider (*e.g.*, third-party service such as Google or Yahoo), authentication of the user of the second client device (*e.g.*, when the email recipient clicks "Sign in with Google" and provides his

YouTube (Sept. 28, 2017), https://www.youtube.com/watch?v=R3cDOFXToNQ&t=1087s.
[92] *Id.*
[93] *Id.*
[94] *Id.*

or her username and password, Microsoft server automatically requests identity authentication from Google).[95]

164. On information and belief, the Accused Products with OME send, by the access control management system (*e.g.*, Microsoft server), to the second client device (*e.g.*, an email recipient's device), the received information associated with the encrypted data object (*e.g.*, the metadata associated with the encrypted email), responsive to the authentication by the selected identity provider of the user of the second client device (*e.g.*, after the recipient successfully signs in, the Microsoft server sends the metadata associated with the encrypted email to the recipient).[96]

165. On information and belief, the Accused Products with OME store, by the access control management system (*e.g.*, Microsoft server), in a transaction log, an identification of at least one of the second client device and the received request for the information (*e.g.*, Microsoft in its protection usage logs, stores information about requests for protected emails).[97]

166. On information and belief, Microsoft has specifically intended, and continues to specifically intend, its customers to use the Accused Products with OME in a manner that infringes at least claim 1 of the '021 Patent. Microsoft has intentionally encouraged, instructed, and/or directed infringing use through training videos, demonstrations, brochures, user guides, and technical documentation.[98]

Infringement of Claim 1 of '021 Patent by Accused Products with AP

167. The Accused Products with AP employ the method of at least claim 1 of the '021

[95] *Id.*
[96] *Id.*
[97] *See, e.g.*, *Logging and analyzing the protection usage from Azure Information Protection*, Microsoft (Mar. 1, 2022), https://docs.microsoft.com/en-us/azure/information-protection/log-analyze-usage.
[98] *See, e.g.*, *Message Policy and Compliance: Office 365 Message Encryption*, Microsoft (Apr. 8, 2021), https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/message-policy-and-compliance?redirectedfrom=MSDN#bkmk_O365_MessageEncryption; Microsoft Ignite, *Protect and control your sensitive emails with new Office 365 Message Encryption capabilities*, YouTube (Sept. 28, 2017), https://www.youtube.com/watch?v=R3cDOFXToNQ&t=1087s.

Patent for sharing secure information with authenticated recipients, in which the authentication is performed by an identity provider that is automatically selected based on information about the authorized recipients, and when information about the authenticated recipients is stored in a transaction log.

168. On information and belief, the Accused Products with AP practice a method for distributing cryptographic data to authenticated recipients via secured or unsecured channels. For example, on information and belief, the Accused Products with AP allow the sharing of a "company's applications and services with guest users from any other organization, while maintaining control over [its] own corporate data."[99]

169. On information and belief, the Accused Products with AP receive, by an access control management system (*e.g.*, Microsoft server), from a first client device (*e.g.*, a device of a user in an Azure tenant using Azure Portal and B2B) information associated with an encrypted data object (*e.g.*, a list of the users allowed to access a particular application where an encrypted data object resides and access permissions for the users).[100]

170. On information and belief, the Accused Products with AP receive, by the access control management system (*e.g.*, Microsoft server), from a second client device (*e.g.*, a device of a guest user), a request for the information associated with the encrypted data object (*e.g.*, an invited guest user clicks on a redemption link in an invitation email, thereby sending a request to the Microsoft server to access the list of the users allowed to access the particular application where the encrypted data object resides and the access permissions for the users).[101]

---

[99] *What Is Guest User Access in Azure Active Directory B2B?*, Microsoft (Oct. 22, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b.

[100] Microsoft Mechanics, *Azure Active Directory B2B Collaboration: simple, secure external sharing of your Apps and Services*, YouTube (Apr. 12, 2017), https://youtu.be/AhwrweCBdsc?t=383; *Restrict guest access permissions in Azure Active Directory*, Microsoft (Dec. 29, 2021), https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-restrict-guest-permissions.

[101] *The elements of the B2B collaboration invitation email – Azure Active Directory*, Microsoft (Jul. 2, 2021),

171. On information and belief, the Accused Products with AP verify, by the access control management system (*e.g.*, Microsoft server), that a user of the second client device (*e.g.*, a guest user) is identified in the received information associated with the encrypted data object (*e.g.*, the Microsoft server verifies that the guest user was invited and is among the list of the users allowed to access the particular application where the encrypted data object resides).[102]

172. On information and belief, the Accused Products with AP automatically select, by the access control management system (*e.g.*, Microsoft server), an identity provider from a plurality of identity providers (*e.g.*, third-party service such as Google or another federated service), based on a user identifier included in the received information associated with the encrypted data object, the user identifier associated with the user of the second client device (*e.g.*, Microsoft server makes a selection of the identity provider automatically based on the email address of the authorized guest user).[103]

173. On information and belief, the Accused Products with AP automatically request, by the access control management system (*e.g.*, Microsoft server), from the selected identity provider (*e.g.*, third-party service such as Google or another federated service), authentication of the user of the second client device (*e.g.*, when the guest user clicks on the redemption link and provides his or her username and password, Microsoft server automatically requests identity authentication from Google).[104]

---

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/invitation-email-elements.

[102] *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133.

[103] *Id.*; *Azure Active Directory B2B collaboration invitation redemption*, Microsoft (Dec. 14, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/redemption-experience.

[104] *Id.*; *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133; Microsoft Security, *Manage partner access with Azure AD B2B collaboration*, YouTube (Aug. 20, 2020), https://youtu.be/AO-uTWSmU_E?t=308.

174. On information and belief, the Accused Products with AP send, by the access control management system (*e.g.*, Microsoft server), to the second client device (*e.g.*, a guest user's device), the received information associated with the encrypted data object, responsive to the authentication by the selected identity provider of the user of the second client device (*e.g.*, after the recipient successfully signs in, the guest user can access the list of the users allowed to access the particular application where the encrypted data object resides and access permissions for the users).[105]

175. On information and belief, the Accused Products with AP store, by the access control management system (*e.g.*, Microsoft server), in a transaction log, an identification of at least one of the second client device and the received request for the information (*e.g.*, Microsoft in its Azure AD audit logs, stores records of system and user activities).[106]

176. On information and belief, Microsoft has specifically intended, and continues to specifically intend, its customers to use the Accused Products with AP in a manner that infringes at least claim 1 of the '021 Patent. Microsoft has intentionally encouraged, instructed, and/or directed infringing use through training videos, demonstrations, brochures, user guides, and technical documentation.[107]

Infringement of Claim 1 of '021 Patent by Accused Products with AKV

177. The Accused Products with AKV employ the method of at least claim 1 of the '021 Patent for sharing secure information with authenticated recipients, in which the authentication is

[105] *See, e.g.*, *What are the default user permissions in Azure Active Directory?*, Microsoft (Dec. 22, 2021), https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions.
[106] *Auditing and reporting a B2B collaboration user, Microsoft (Aug. 6, 2020)*, https://docs.microsoft.com/en-us/azure/active-directory/external-identities/auditing-and-reporting.
[107] *See, e.g.*, *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133; Microsoft Security, *Manage partner access with Azure AD B2B collaboration*, YouTube (Aug. 20, 2020), https://youtu.be/AO-uTWSmU_E?t=308.

performed by an identity provider that is automatically selected based on information about the authorized recipients, and when information about the authenticated recipients is stored in a transaction log.

178. On information and belief, the Accused Products with AKV practice a method for distributing cryptographic data to authenticated recipients via secured or unsecured channels. For example, on information and belief, the Accused Products with AKV allow the sharing of "keys, secrets, and certificates stored in [Azure Key Vault]" with "users both within an organization and outside."[108]

179. On information and belief, the Accused Products with AKV receive, by an access control management system (*e.g.*, Microsoft server), from a first client device (*e.g.*, a device of a user in an Azure tenant using Azure Key Vault and B2B) information associated with an encrypted data object (*e.g.*, a cryptographic key that is used to encrypt an encrypted data object, a list of the users allowed to access the Azure Key Vault where the cryptographic key resides, and access permissions for the users).[109]

180. On information and belief, the Accused Products with AKV receive, by the access control management system (*e.g.*, Microsoft server), from a second client device (*e.g.*, a device of a guest user), a request for the information associated with the encrypted data object (*e.g.*, an invited guest user clicks on a redemption link in an invitation email, thereby sending a request to the Microsoft server to access the cryptographic key that is used to encrypt the encrypted data

[108] *Secure Your Sensitive Business Information with Azure Key Vault*, Microsoft (Jan. 4, 2019), https://docs.microsoft.com/en-us/archive/msdn-magazine/2018/march/azure-secure-your-sensitive-business-information-with-azure-key-vault.

[109] *Assign a Key Vault access policy*, Microsoft (Sep. 10, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal; *Provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control*, Microsoft (Oct. 16, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli; Microsoft Security, Azure Key Vault: What's new, YouTube (Sep. 22, 2020), https://youtu.be/d8Xv6PJEfPw?t=137.

object, the list of the users allowed to access the Azure Key Vault where the cryptographic key resides, and the access permissions for the users)[110].

181. On information and belief, the Accused Products with AKV verify, by the access control management system (*e.g.*, Microsoft server), that a user of the second client device (*e.g.*, a guest user) is identified in the received information associated with the encrypted data object (*e.g.*, the Microsoft server verifies that the guest user was invited and is among the list of the users allowed to access the Azure Key Vault where the cryptographic key that is used to encrypt the encrypted data object resides).[111]

182. On information and belief, the Accused Products with AKV automatically select, by the access control management system (*e.g.*, Microsoft server), an identity provider from a plurality of identity providers (*e.g.*, third-party service such as Google or another federated service), based on a user identifier included in the received information associated with the encrypted data object, the user identifier associated with the user of the second client device (*e.g.*, Microsoft server makes a selection of the identity provider automatically based on the email address of the authorized guest user).[112]

183. On information and belief, the Accused Products with AKV automatically request, by the access control management system (*e.g.*, Microsoft server), from the selected identity provider (*e.g.*, third-party service such as Google or another federated service), authentication of the user of the second client device (*e.g.*, when the guest user clicks on a redemption link and provides his or her username and password, Microsoft server automatically requests identity

[110] *The elements of the B2B collaboration invitation email – Azure Active Directory*, Microsoft (Jul. 2, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/invitation-email-elements.
[111] *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133.
[112] *Id.*; *Azure Active Directory B2B collaboration invitation redemption*, Microsoft (Dec. 14, 2021), https://docs.microsoft.com/en-us/azure/active-directory/external-identities/redemption-experience.

authentication from Google)).[113]

184. On information and belief, the Accused Products with AKV send, by the access control management system (*e.g.*, Microsoft server), to the second client device (*e.g.*, a guest user's device), the received information associated with the encrypted data object, responsive to the authentication by the selected identity provider of the user of the second client device (*e.g.*, after the guest user successfully signs in, the guest user can access the cryptographic key that is used to encrypt the encrypted data object, the list of the users allowed to access the Azure Key Vault where the cryptographic key resides, and the access permissions for the users)[114].

185. On information and belief, the Accused Products with AKV store, by the access control management system (*e.g.*, Microsoft server), in a transaction log, an identification of at least one of the second client device and the received request for the information (*e.g.*, Microsoft in its Key Vault logs, stores information about when and how key vaults are accessed).[115]

186. On information and belief, Microsoft has specifically intended, and continues to specifically intend, its customers to use the Accused Products with AKV in a manner that infringes at least claim 1 of the '021 Patent. Microsoft has intentionally encouraged, instructed, and/or directed infringing use through training videos, demonstrations, brochures, user guides, and technical documentation.[116]

---

[113] *Id.*; *Azure AD B2B collaboration direct federation with SAML and WS-Fed providers now in public preview*, Alex Simons (AZURE) (Jul. 8, 2019), https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-b2b-collaboration-direct-federation-with-saml-and-ws/ba-p/735133; Microsoft Security, *Manage partner access with Azure AD B2B collaboration*, YouTube (Aug. 20, 2020), https://youtu.be/AO-uTWSmU_E?t=308.

[114] *See, e.g.*, *Azure Key Vault security*, Microsoft (Dec. 9, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/security-features.

[115] *Azure Key Vault logging,* Microsoft (Dec. 28, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/logging?tabs=Vault.

[116] *See, e.g.*, *Secure Your Sensitive Business Information with Azure Key Vault*, Microsoft (Jan. 4, 2019), https://docs.microsoft.com/en-us/archive/msdn-magazine/2018/march/azure-secure-your-sensitive-business-information-with-azure-key-vault; *Assign a Key Vault access policy*, Microsoft (Sep. 10, 2021), https://docs.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal.

PRAYER FOR RELIEF

WHEREFORE, Virtru respectfully requests that this Court enter judgment in its favor and grant the following relief:

(a) A judgment that Microsoft has directly and/or indirectly infringed one or more claims of each of the Patents-in-Suit;

(b) A judgment for a permanent injunction against Microsoft and its respective officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all other acting in active concert therewith from infringement of the Patents-in-Suit;

(c) A judgment and order requiring Microsoft to pay Virtru past and future damages under 35 U.S.C. § 284, including for supplemental damages arising from any continuing post-verdict infringement for the time between trial and entry of the final judgment with an accounting, as needed, as provided by 35 U.S.C. § 284;

(d) A judgment and order requiring Microsoft to pay Virtru reasonable ongoing royalties on a going-forward basis after final judgment;

(e) A judgment and order requiring Microsoft to pay Virtru pre-judgment and post-judgment interest on the damages award;

(f) A judgment and order that Microsoft's infringement of the Patents-in-Suit be found willful and that the Court award treble damages pursuant to 35 U.S.C. § 284;

(g) A judgment that this case be found exceptional under 35 U.S.C. § 285, and an order awarding to Virtru its attorneys' fees incurred in prosecuting this action;

(h) A judgment and order requiring Microsoft to pay Virtru's costs and expenses incurred in prosecuting this action; and

(i) Such other and further relief, including equitable relief, as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Virtru requests a trial by jury of any issues so triable by right.

Dated: March 4, 2022

Respectfully submitted,

Richard D. Milvenan (Bar No. 14171800)
Ian M. Davis (Bar No. 24120793)
McGINNIS LOCHRIDGE LLP
1111 W. 6th Street, Bldg. B, Suite 400
Austin, TX 78703
Phone: (512) 495-6000
Fax: (512) 495-6093
Email: rmilvenan@mcginnislaw.com
Email: idavis@mcginnislaw.com

/s/Richard D. Milvenan
Richard D. Milvenan

ATTORNEY FOR
PLAINTIFF VIRTRU CORPORATION

OF COUNSEL:

MORRISON & FOERSTER LLP

Mark L. Whitaker (*pro hac vice* application to be filed)
D.C. Bar No. 435755
MWhitaker@mofo.com
Mary Prendergast (*pro hac vice* application to be filed)
D.C. Bar No. 1034426
MPrendergast@mofo.com
Fitz B. Collings (*pro hac vice* application to be filed)
D.C. Bar No. 1015729
FCollings@mofo.com
2100 L Street, NW, Suite 900
Washington, District of Columbia 20037
Telephone: (202) 887-1500
Facsimile: (202) 887-0763

Rudy Y. Kim (*pro hac vice* application to be filed)
California State Bar No. 199426
RudyKim@mofo.com
755 Page Mill Road
Palo Alto, California 94304-1018
Telephone: (650) 813-5600
Facsimile: (650) 494-0792

Shaelyn K. Dawson (*pro hac vice* application to be filed)
California State Bar No. 288278
ShaelynDawson@mofo.com
425 Market Street
San Francisco, California 94105
Telephone: (415) 268-7000
Facsimile: (415) 268-7522

ATTORNEYS FOR
PLAINTIFF VIRTRU CORPORATION